
دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية



الجرائم الإلكترونية والإنترنت

د. فريجه حسين
أستاذ محاضر
جامعة المسيلة-الجزائر

المقدمة :

توسعت شبكة الإنترنت ولم تعد قاصرة على أغراض البحث العلمي بل امتدت لتشمل المعاملات التجارية وظهرت جرائم على الشبكة ازدادت مع الوقت وتعددت صورها وأشكالها، وهذه الجرائم تطلق عليها الجرائم الإلكترونية أي تلك الأعمال التي تتم عن طريق الإنترنت.

والتطور المستمر للإنترنت وتوفر السرية التامة جعلاً من الإنترنت جهازاً لتنفيذ العديد من الجرائم بعيدا عن أعين الجهات الأمنية، فقد سمحت شبكة الإنترنت لظهور الجرائم الإلكترونية. وأصبح الإنترنت نموذجاً صارخاً للإجرام فيه ثغرات قانونية تتحدى الأجهزة الأمنية والقضائية.

إن ظاهرة الجريمة الإلكترونية ظاهرة حديثة يقترفها مجرمون أذكياء يمتلكون قوة المعرفة الفنية والتقنية. والجريمة الإلكترونية تمس الحياة الخاصة للأفراد وتهدد الأعمال التجارية بخسائر فادحة كما تنال من الأمن القومي والسيادة. [1]

إن الجريمة الإلكترونية امتدت وتوسعت إلى التشهير بالشخص وتشويه السمعة وجرائم النصب والاحتيال وغيرها من الأفعال الإجرامية. [2]

المبحث الأول : ماهية الجريمة الإلكترونية وخصائصها

سنتعرض الأول: المبحث إلى مفهوم الجريمة الإلكترونية والأداة المستعملة لارتكاب هذه الجريمة في مطلب أول، أما المطلب الثاني فسنخصصه إلى خصائص الجريمة الإلكترونية.

المطلب الأول : تعريف الجريمة الإلكترونية وأداتها

هي الجريمة ذات الطابع المادي تتمثل في كل فعل أو سلوك غير مشروع مرتبط بأية وجهة بالحاسبات، يتسبب في تكبد أو إمكانية تكبد المجني عليه خسارة، وحصول أو إمكانية حصول مرتكبة على أي مكسب ولها مسميات منها جرائم الكمبيوتر والإنترنت – الجريمة الإلكترونية، ونظراً لتطور الجرائم الإلكترونية وتعدد أشكالها وأنواعها كلها أوغل العالم وتمعن في استخدام الحاسب مما أدى إلى صعوبة حصرها ووضع نظام قانوني يخضع له المجرم، حيث يمكن ارتكاب الجريمة بضغطة زر وصعوبة تحديد الفاعل أو عدم إمكانية معرفة مكانه أدى إلى إثارة الجدل حول الجرائم الإلكترونية. [3]

إن الكمبيوتر له صلة وثيقة بالجرائم الإلكترونية، فلا جريمة الكترونية دون حاسب، فالحاسب له دور أساسي في مجال الجريمة الإلكترونية. فيقوم الحاسب بعدة أدوار في حالة ارتكاب الجريمة.

1– يكون الكمبيوتر هدفاً للجريمة، مثل حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات أو الملفات المخزنة أو تعطيلها أو لزم استخدام وسائل متطورة لاكتشاف الجرائم ومن هنا يلعب الكمبيوتر دوراً رئيسياً في كشف الجرائم وتتبع فاعليها بل وإبطال الهجمات التدميرية لمخترقي النظم وتحديداً هجمات الفيروسات وقرصنة البرمجيات. الاستيلاء على البيانات المخزنة أو المنقولة. [4]

2– يكون الكمبيوتر أداة لارتكاب الجريمة .

3– الكمبيوتر يكون بيئة الجريمة، كحالة استخدامه لنشر المواد غير القانونية أو استعماله كأداة لترويج المخدرات أو نشر الشبكات الإباحية.

أما دور الكمبيوتر في حالة اكتشاف الجريمة، فهو يستخدم في التحقيق لجميع الجرائم، كما أن تنفيذ القانون يعتمد على النظم التقنية من خلال تطبيق القانون ومع تزايد ارتكاب جرائم الكمبيوتر واعتماد مرتكبيها على وسائل متجددة ومتطورة.

المطلب الثاني : خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بخصائص تميزها عن الجريمة التقليدية تتمثل فيما يلي:

أولاً : الجريمة الإلكترونية عابرة للحدود

الجريمة الإلكترونية تتسم بالطابع الدولي، لأن نظام الإنترنت جعل من معظم دول العالم في حالة اتصال دائم على الخط . فالجريمة الإلكترونية لا تعترف بالحدود بين الدول وبالتالي فهي شكلاً جديداً من أشكال الجرائم العابرة للحدود بين الدول، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل جرائم التعدي على البيانات وتزوير وإتلاف المستندات الإلكترونية والاحتيال المعلوماتي والقرصنة وسرقة الأموال.

إن قدرة الإنترنت على اختصار المسافات، انعكست على طبيعة الأعمال الإجرامية ولم تعد الجريمة محلية بل أصبحت عالمية، والجريمة الإلكترونية يرتكبها صاحبها عن بعد وهو يعني عدم التواجد المادي للجرم المعلوماتي في مكان الجريمة. ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر وبين النتيجة أي المعطيات. والجريمة الإلكترونية تنتقل من دولة لأخرى. [5]

وتعتبر الجريمة الإلكترونية صورة صادقة عن العولمة، فيمكن ارتكاب هذه الجريمة عن بعد، وقد يتعد ارتكابها بين أكثر من دولة، كما أن المواقيت تختلف بين الدول مما يثير إشكالية حول القانون الواجب التطبيق على هذه الجريمة.

ثانياً : صعوبة إثبات الجريمة الإلكترونية

تتصف هذه الجريمة بالخفاء أي عدم وجود آثار مادية يمكن متابعتها وهي صعبة الاكتشاف، كما أنه من الصعوبة تحديد مكانفحصها. وترجع صعوبة إثبات الجريمة المعلوماتية إلى عدة عوامل منها:

1- أن الجريمة الإلكترونية لا تترك آثار مادية، فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية ولا توجد مستندات ورقية. فهذه الجريمة عبارة عن أرقام تتغير في السجلات فالجريمة الإلكترونية لا تترك شهوداً يمكن استجوابهم ولا أدلة يمكن فحصها .

2- صعوبة الاحتفاظ بدليل الجريمة الإلكترونية، إذ يستطيع المجرم في أقل من ثانية أن يمحو أو يحرف أو يغير المعلومات الموجودة في الكمبيوتر. [6]

3- تحتاج الجريمة الإلكترونية لاكتشافها إلى خبرة فنية، حيث تتطلب جريمة الكمبيوتر إلمام ومعلومات واسعة سواء لارتكابها أو التحقيق فيها. كما أن رجال الضبطية القضائية يجدون صعوبة للتعامل مع الدليل الإلكتروني، فقد يتسبب المحقق بدون قصد في إتلاف الدليل الإلكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة الصلبة أو قد لايقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو الطابعة أو الماسح الضوئي. لذلك أصبح من الضروري في وقتنا إجراء دورات تدريبية لرجال الضبطية القضائية ورجال القضاء والخبراء والفنيين للتعاون فيما بينهم وصولا إلى أحسن الطرق لمكافحة الجريمة الإلكترونية. [7]

4- تعتمد الجريمة الإلكترونية على الخداع والذكاء في التعرف على مرتكبيها إن الذي يساعد على عدم التعرف على مرتكبي الجرائم الإلكترونية إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم تجنبا للإساءة إلى سمعتها وهز ثقة العملاء بها، وإخفاء أسلوب ارتكاب الجريمة خوفاً من قيام الآخرين بتقليد هذا الأسلوب، وهو ما يدفع المجني عليه إلى الإحجام عن إبلاغ السلطات المختصة بها. كما أن الجريمة المعلوماتية تعتمد على الذكاء وهي جريمة فردية تعتمد على مهارات عالية وإلمام بتكنولوجيا النظم المعلوماتية.[8]، وتقع الجريمة المعلوماتية أثناء معالجة البيانات والمعطيات الخاصة بالكمبيوتر وإذا تخلف هذا الشرط تنتفي الجريمة.

وقد حاول مجلس الشيوخ في فرنسا وضع تعريف محدد لعملية المعالجة الآلية للبيانات أو المعطيات ولكنه عدل عنه باعتبار أن هذه الجريمة عملية فنية تخضع للتطور السريع وبالتالي أي تعريف لها سيكون ناقصاً. [9] وكان هذا التعريف ينص على " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات والتي يتم عن طريقها تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام الحماية الفنية " .

والجريمة المعلوماتية تقع أثناء المعالجة الآلية للبيانات في مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج المعلومات.

ففي مرحلة إدخال المعلومات، تترجم المعلومات إلى لغة مفهومة من قبل الآلة يكون من السهل إدخال بيانات لا علاقة لها تماماً بالمعطيات الأساسية ومحو البيانات المطلوب إدخالها.

وفي مرحلة المعالجة حيث يمكن إدخال بيانات غير مصرح بها واستبدالها بالبيانات الأساسية أو تشغيل برامج جديدة تلغي عمل البرامج الأصلية جزئياً أو كلياً.

أما المرحلة الأخيرة فيتم التلاعب بالنتائج التي يخرجها النظام المعلوماتي تتمثل في بيانات غير صحيحة أدخلت فيها معالجة غير صحيحة. [1]

المبحث الثاني : الجرائم المرتكبة باستخدام النظام المعلوماتي

تتنوع الجرائم التي ترتكب بواسطة النظام المعلوماتي ما بين جرائم اقتصادية أو قرصنة المعلومات أو ذات طابع سياسي أو متعلقة بالأمن القومي وقد تقع هذه الجرائم على الأشخاص الطبيعية أو الاعتبارية. [10]

المطلب الأول : جرائم الأموال

وهذه الجرائم تتمثل خاصة في جرائم التجارة الإلكترونية وجرائم التحويل الإلكتروني للأموال وجريمة غسيل الأموال عبر الإنترنت وجريمة إتلاف المعلومات المبرمجة آليا.

وسنتناول هذه الجرائم كما يلي:

الفرع الأول: جريمة التجارة الإلكترونية

شاعت وانتشرت التجارة الإلكترونية التي تتيح لرجال الأعمال تجنب مشقة السفر والانتقال من بلد إلى آخر للقاء شركائهم وعملائهم وأصبح بمقدورهم توفير الوقت والجهد والمال، كما أصبح في متناول المستهلك الحصول على ما يريده دون التنقل أو استخدام النقود التقليدية وكل ما يحتاجه المستهلك هو اقتناء جهاز كمبيوتر وبرنامج مستعرض للإنترنت واشتراك بشبكة الإنترنت. [11]

كما أن التجارة الإلكترونية منذ بدايتها كانت تتضمن معالجة حركات البيع والشراء وتحويل الأموال إلكترونيا عبر شبكة الإنترنت، فالتجارة الإلكترونية هي نظام يتيح عبر شبكة الإنترنت حركات بيع وشراء وتأجير السلع والخدمات والمعلومات. ويمكن تشبيه التجارة الإلكترونية بسوق إلكتروني يتقابل فيه البائعون والموردون والمستهلكون وتقدم فيه المنتجات والخدمات في صورة رقمية أو افتراضية ويتم دفع ثمنها بالنقود الإلكترونية. [12]

والتجارة الإلكترونية عرفت قفزة هائلة في سنة 2006 وبلغت قيمة المعاملات في الولايات المتحدة وحدها مائة مليار دولار. [13]

وقد ازداد حجم الجرائم المرتكبة ضد التجارة الإلكترونية لأن الوفاء يتم عن طريق بطاقات الائتمان، كما ظهرت جرائم السطو والقرصنة على البيانات الشخصية عبر الإنترنت.

ومن جرائم التجارة الإلكترونية الجرائم التي ترتكب ضد المستهلك إذ يستطيع المستهلك التعامل في الأسواق المحلية والعالمية بضغطة واحدة على جهاز الكمبيوتر لطلب السلعة أو الخدمة المعروضة وأصبحت الإعلانات تؤثر على المستهلك ويبنى عليها قراره في الإقبال على التعاقد. فإذا كانت الرسالة الإعلانية كاذبة أو مضللة فإنها بلا شك تؤثر على المستهلك.

الفرع الثاني : جرائم التحويل الإلكتروني للأموال

نظام التحويل الإلكتروني للأموال هو بالغ الأهمية للبنوك التي تعمل عبر الإنترنت، ويتيح هذا النظام بطريقة إلكترونية آمنة تحويل المال من حساب بنكي إلى حساب آخر.

ونظام التحويل الإلكتروني للأموال يقصد منه منح الصلاحية لأحد البنوك للقيام بحركات التحويلات المالية الدائنة والمدينة إلكترونيا من حساب بنكي إلى حساب بنكي آخر .

وقد عرفت لجنة الأمم المتحدة للقانون التجاري الدولي المقصود بنظام التحويل الإلكتروني للأموال بأنه " عملية تبادل القيم المادية والتي تتم مرحلة بها أو أكثر بواسطة وسائل إلكترونية بعد أن كانت نفس هذه المرحلة تتم قديما بالوسائل الكتابية التقليدية. [14]

ومن أبرز شبكة التحويلات المالية شبكة السويفت (swift) وهو نظام يستخدم على نطاق واسع في البنوك الوطنية، لتسوية المدفوعات المالية بالوسائل الإلكترونية. ويتم ذلك بتوجيه أمر من المدين إلى بنكه بالوفاء من حسابه إلى دائنه إلكترونياً، باتخاذ الإجراءات المصرفية اللازمة لتحويل مبلغ معين لحساب بنك المستفيد، أو بتوجيه الدائن أمرا إلى بنكه بتحصيل مبلغ من حساب مدينه بناء على تفويض مسبق بواسطة إلكترونية. [15] تتم بواسطة نظام التحويل الإلكتروني للأموال. [16]

ومن صور التعدي على نظام التحويل الإلكتروني للأموال ما أشار إليه التقرير الصادر عن إدارة العدالة الأمريكية لعام 1982. بعنوان جرائم الحاسب الآلي نظم التحويل الإلكتروني للأموال. [17]

ويتم التلاعب في نظام التحويل الإلكتروني للأموال بأي وسيلة من وسائل الاحتيال المعلوماتي، حيث يتم التلاعب عند إدخال البيانات أو في برامج الكمبيوتر أو في المكونات المادية له أو أثناء عملية نقل البيانات إلكترونياً.

الفرع الثالث : جريمة غسيل الأموال إلكترونياً

هذه الجريمة ترتكب عبر النظام الإلكتروني وهي عملية يقصد بها نقل أموال مستمدة من مصدر غير مشروع بقصد تطهيرها، فعملية التحويل الإلكتروني لهذه الأموال لا يشوبها أي تلاعب إلا أن صفة عدم المشروعية يرجع إلى مصدر هذه الأموال ذاتها. وتتم عبر الانترنت عن طريق البنوك حيث تتم العمليات المصرفية بطريقة الكترونية سريعة.

وتعرف جريمة غسيل الأموال بأنها:" مجموعة عمليات معينة ذات طبيعة اقتصادية أو مالية تؤدي إلى إدخال الأموال دائرة الاقتصاد الشرعي رؤوس أموال ناتجة من أنشطة غير مشروعة تقليديا متعلقة بالمتاجرة بالمخدرات واليوم أصبحت نواتج كل جريمة جنائية ذات جسامة أو خطورة ". [18]

وقد تعددت المصطلحات الدالة على عمليات غسيل الأموال منها مصطلح غسيل الأموال القذرة، مصطلح تبييض الأموال .

وقد أصدر المشرع الجزائري قانونا يتعلق بجريمة غسيل الأموال وسماها تبييض الأموال. [19] وهذه الجرائم تكون متأتية خاصة من جرائم المخدرات وجرائم الإرهاب واستيراد الأسلحة والدعارة ...الخ

وتمر عملية غسيل الأموال بالمراحل التالية:

1- مرحلة الإيداع أو التوظيف، وفيها يتم إيداع الأموال الناتجة عن أعمال غير مشروعة في شركات مالية أو بنوك، الأمر الذي يعني إيداع الأموال غير المشروعة في مؤسسات أو بنوك.

2- مرحلة التقييم والتمويه، وفيها يتم إجراء سلسلة من العمليات لإخفاء الأصل غير المشروع للأموال، حيث يقوم غاسل الأموال بخلق مجموعات مضاعفة من الصفقات التجارية والتحويلات المالية مثل الاستثمار في عدة دول أجنبية.

3– مرحلة الإدماج، وتهدف هذه المرحلة إلى إضفاء الشرعية على تلك الأموال وتعاد الأموال مرة أخرى في شكل عوائد نظيفة وغير خاضعة للضرائب. [20]

الفرع الرابع: جريمة إتلاف المعلومات الإلكترونية

تستخدم كلمة فيروس للدلالة على كل البرامج الخبيثة التي تسبب إتلافاً لأنظمة المعالجة ويوجد منها أنواع كثيرة مثل فيروس الدودة وحصان طروادة، والقنبلة الموقوتة (المنطقية) وهذه تتسبب في إتلاف المكونات المنطقية للحاسب الآلي أو تعطيل شبكات الكمبيوتر عن تأدية مهامها. [21] وتتنوع الفيروسات التي تصيب المعلومات كالآتي:

1 **حصان طروادة**: وهو عبارة عن برمجية اختراق من حيث التقنية، فهو يختبئ داخل البرامج الموجودة بالذاكرة ثم ينشط في الوقت المحدد له وينفذ الأمر المعطى له إما بتعديل في البرنامج أو الإتلاف نهائياً أو يقوم بمحو البيانات أو تشويهها، وقد ظهرت أولى جرائم حصان طروادة في انجلترا عام 1989 عندما قام شخص يدعى الدكتور " بوب " من أوهايو بالولايات المتحدة الأمريكية حيث كان يستخدم أسلوب إرسال حصان طروادة في ديسكات حول العالم لارتكاب جرائم ابتزاز، ولقد تضرر من عمله حوالي 20 ألفاً في مدينة لندن بانجلترا.

2 **فيروس الدودة**: وهو عبارة عن برمجية تقوم بالانتقال من حاسوب إلى آخر دون حاجة إلى تدخل إنساني لتنشيطها، وبخاصة التنشيط الذاتي، وبهذا تختلف الدودة عن حصان طروادة إلا أنها لا تلتصق بنظام التشغيل في الحاسوب الذي تصيبه وتتسبب حركة الدودة في تعطيل الحاسوب بتجميد لوحة المفاتيح والشاشة وتعبئه الذاكرة وتبطئة الحاسوب.

وقد ظهرت الدودة على يد " موريس " طالب الدكتوراه في علوم الحاسب بجامعة كورنل وتم برمجة دودة موريس على أن تطبع ذاتها عند تلقيها للإجابة السابقة المؤكدة. وقد انزلقت الدودة إلى نظام البريد الإلكتروني عبر ثغرة فيه تركت بقصد تسهيل عملية الدخول إليه لإصلاحه حال وجود خلل ما ولقد حطمت دودة موريس كلمات المرور وانتشرت في جميع الحواسيب. [22]

3 **القنبلة الموقوتة (المنطقية)** : وهو عبارة عن فيروس يظل ساكتا حتى حدوث واقعة معينة أو كلمة محددة قد يكتبها المستخدم أو تاريخ معين يبدأ في عمله من خلال موقعه على الذاكرة ثم ينشط ويقوم بتدمير البرامج أو تدمير قوائم العمال أو الزبائن .

المطلب الثاني : جرائم الأشخاص

نحاول أن نعرض بعض الجرائم التي ترتكب بواسطة النظام المعلوماتي عن طريق الانترنت وتتمثل هذه الجرائم خاصة في جرائم السب والقذف عبر الانترنت، وجرائم التعدي على الحياة الخاصة، والجرائم المخلة بالآداب العامة عبر الانترنت.

الفرع الأول : جرائم السب والقذف عبر الانترنت

عرفت المادة 297 من قانون العقوبات الجزائري السب بقولها: " يعد سباً كل تعبير مشين أو عبارة تتضمن تحقيراً أو قدحاً لا ينطوي على إسناد واقعة ".

كما يعرف القذف بأنه :" إسناد واقعة محددة تستوجب عقاب من تنسب إليه أو احتقاره إسناداً علناً عموديا يفيد نسبة الأمر إلى الشخص على سبب التوكيد ". ويعرف السب بأنه:" خدش شرف شخص واعتباره عمداً دون أن يتضمن ذلك إسناد واقعة معينة إليه ".

فالفرق بين السب والقذف أن القذف يتضمن إسناد واقعة محددة إلى الشخص في حين أن السب لا يتضمن ذلك. [23]

ويتضح من النصوص السابقة أن السب والقذف يتطلبان بكل وضوح العلنية كما نص القانون على ذلك صراحة. وهو مايعني: نشر السب والقذف عن طريق الانترنت تتحقق به العلانية.

الفرع الثاني : جرائم التعدي على الحياة الخاصة

الحياة الشخصية الخاصة تحظى بحماية دستورية وقانونية فقد عني المشرع الجزائري بإضفاء الحماية على الحياة الخاصة سواء بالدستور أو بالقانون وقد يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة، كما لو قام شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص بدون علمه وبغير إذنه وقام هذا الشخص بإطلاع الغير عليها بدون إذن صاحبها كما في حالة الأسرار المودعة لدى المحاسبين أو لدى المحامين أو لدى الأطباء فكل هذه الأسرار يحميها القانون ويجرم إفشاءها بالطرق غير المشروعة وبدون موافقة صاحبها. وجريمة التعدي على الحياة الخاصة والإطلاع على الأسرار أو إفشاءها قد تتم بنشر المعلومات على الكمبيوتر وفتح السجلات الإلكترونية والإطلاع عليها من خلال شاشة الكمبيوتر.

ويدخل في نطاق جرائم التعدي على الحياة الخاصة جريمة تسجيل المحادثات الشخصية أو مراقبتها بأية وسيلة حيث نجد بعض المتسللين يستطيعون اختراق شبكة الانترنت بطرق غير مشروعة والتصنت على هذه المكالمات.

والسر يعتبر معلومة أو خبر، والإفشاء جوهره نقل المعلومات وهو نوع من الأخبار ويعني الإطلاع من الغير على المعلومة التي تعتبر نوع من السر الشخصي الذي لا يرغب صاحبه في إطلاع الغير عليه وإرادته الاحتفاظ بهذا السر في حيز الكتمان، وهذه الرغبة هي التي يحترمها المشرع وهي علة تجريم إفشاء الأسرار عن طريق الانترنت. [24]

الفرع الثالث : الجرائم المخلة بالآداب العامة عبر الانترنت

وجد العاملون في مجال الإباحية ونشر الصور الخليعة في شبكة الانترنت وسيلة ذات كفاءة عالية وجاذبية وإغراء في الدعوة إلى ممارسة الفجور والبغاء وذلك عن طريق الإعلانات الإلكترونية عبر المواقع المنتشرة على شبكة الانترنت وذلك كله في إطار التقنية الفنية التي يستخدمها الجاني في ارتكابه للجريمة وصعوبة اكتشاف هذه الجرائم وتحديد مصدرها وإقامة الدليل عليها، بالإضافة إلى غياب التشريعات الحديثة التي تواجه مثل هذه الجرائم الأخلاقية التي ترتكب عبر شبكة الانترنت.

وتتمثل نشر الجرائم المخلة بالآداب العامة والإباحية الجنسية على الانترنت في نشر الصور المخلة والممارسات غير أخلاقية.

ولعل هذا الوضع يتطلب تدخل المشرع الجزائري لمواجهة القصور في التشريعات والقوانين السارية وجعلها مواكبة لعصر التقنية الحالي وذلك بتجريم استخدام شبكة الانترنت والكمبيوتر في الإعلان عن الجرائم المخلة بالآداب.

الهوامش والمراجع :

1. الدكتور خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية 2008 ص 7.
تقرير الأونكتاد 10 نوفمبر 2005 .

2. منيرة بنت فهد الحمدان ، الجرائم الإلكترونية ومكافحتها ، الحاسب أداة الجريمة ، وسيلة اكتشافها ، منشور في الإنترنت .

3. نصت المادة 314 مكرر من قانون العقوبات الجزائري علاالمنظومة،،عاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50000 دج إلى 100,000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك . وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ، إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة من 6 أشهر إلى سنتين ..." .

4. الدكتور خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية – الإسكندرية 2008 ص 44.

5. د . هشام محمد فريد رستم ،" القانون والكمبيوتر والانترنت" بحث مقدم بجامعة دولة الإمارات العربية المتحدة – 1 – 3 – ماي 2000 .

6. تقرير الأونكتاد 10 نوفمبر 2005 ملتقى الأمم المتحدة حول التجارة والتنمية ص 2 .

7. أحمد خليفة الملط – الجرائم المعلوماتية ، دار الفكر الجامعي ، 2005 ص 113 وما بعدها .

8. د . علي عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالأنه:كترونيا ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت – والذي عقد بتاريخ 1 – 3 ماي 2000 كلية الشريعة والقانون – دولة الإمارات العربية ص 42 وما بعدها .

9. د . نائلة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، 2005 ص 106

10. نصت المادة 394 مكرر 3 من قانون العقوبات الجزائري على أنه :" تضاعف العقوبات ... إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام ، دون الإخلال بتطبيق عقوبات أشد " .

11. د . الإبراهيم،براهيم حجازي، سابق ص 68 .

12. د . عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الإلكترونية ، الكتاب الأول – نظام التجارة الإلكترونية وحمايتها مدنيا ، دار الفكر الجامعي 2002 ص 44 .

13. دكتور إإبراهيم، السقا ، جريمة التزوير في المحررات الإلكترونية ، دار الجامعة الجديدة للنشر ، الإسكندرية 2008 ص 22 .

14. د . خالد ممدوح إبراهيم ، مرجع سابق ص 75 .

15. دكتور إيهاب فوزي السقا ، مرجع سابق ص 44 .

16. يقصد بنظام الفريد،الإلكتروني للأموال بمعنى systéme electronic funds transfer –swift

17. د. نائلة عادل محمد فريد ، مرجع سابق ص75.

18. Manacorda (sc)la reglementation du blanchiment de capitaux en droit International du systéme .rev Sc criminelle . 2Avr il 1999 P251.

19. مشار إليه د . خالد ممدوح إبراهيم ، ص 177

20. نصت المادة 389 مكرر من قانون العقوبات على أنه يعتبر تبييض للأموال :

أ – تحويل المتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصادر غير المشروع لتلك المتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه المتلكات، على الإفلات من الآثار القانونية لفعلته.

ب –إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو إجرامية.تعلقة بها، مع علم الفاعل أنها عائدات إجرامية.

ج– اكتساب المتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية .

د– المشارك في أي من الجرائم المقرر وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه.

21. د . محمد سامي الشواء ، السياسة الجنائية في مواجهة غسيل الأموال – دار النهضة العربية – 2002 ص 132

22. د . عصام عبد مطر، ح مطر، الحكومة الإلكترونية بين النظرية والتطبيق، مرجع سابق ص 140 وما بعدها، وأيضا : د. دكتور خالد ممدوح إبراهيم ، مرجع سابق ، ص 73 وما بعدها .

23. د . عصام عبد الفتاح مطر ، الحكومة الإلكترونية بين النظرية والتطبيق ، ص 142 .

24. يبرز نشاط القنبلة الموقوتة في البرقي: ت المؤجرة التي لا يفقد مالكها عليها حقوق الملكية فهو يقوم بتأجيرها فقط ، فإذا توقف المستأجر عن دفع القيمة الإيجارية المنتظمة فإن ذلك يعد إخلالا بالعقد المبرم ويرسل له المالك قنبلة منطقية أو أن تنفجر القنبلة لكون المالك لم يرسل ما يوقف نشاطها .

تتطلب جريمة القذف عدة عناصر تتمثل في :

- تعيين الشخص المقصود .
- تبيان العبارات الماسة بالشرف والاعتبار .
- العلانية .
- صحة الوقائع المسندة .

وقد عرفت المادة 296 من قانون العقوبات الجزائري القذف بأنه: "يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على هذا الإدعاء أو ذلك الإسناد مباشرة ... " .

1– تنص المادة 65 مكرر من ق اج" إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجهورية المختص أن يأذن بما يلي:

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

–وضع الترتيبات التقنية ، دون موافقة المعنيين ، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص

المقدمة: إذن المسلم بغرض الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص في حالة فتح تحقيق قضائي ، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة ... " .